1. **Introduction:**
2. *Background Study:*

With the development of technology, personal data security and privacy is considered as a major challenge for all over the world. Biometrics systems are used to protect data and identity verification [1]. The safety issues of biometric information cannot be compromised. Where the issues have appeared, it may effect on the quality and users' reliability. Some published research papers are related to biometric information privacy [2] and few define the critical issues of biometric information security [3]. A good reliability rate can increase biometric system users rather than using passwords or pin codes and poor reliability will reduce users.

Online banking service [4], employee attendance, employee time tracking device and other identity verification systems are frequently used in Bangladesh. The most common methods of verification fingerprint and face recognition. On 2nd October 2016 Bangladesh government launched the Smart National ID card [5] and started collecting biometric information from the citizens. Recently to digitalize government services, the NID verification gateway server is getting under way [6]. With the large possibility of using biometric technology, it is very important to study the reliability and the trustworthiness of all biometric systems which are used in Bangladesh at users’ point of view.

Most of the biometric systems are integrated with hardware and software. The biometric system market will increase by 15% compound annual growth rate between 2017 and 2023 [7]. The market demand for new biometric systems can be visualized by analyzing adoption, satisfactoriness and reliability reviews.

1. *Research Objectives:*

The aim is to evaluate the biometric systems in terms of system reliability and user satisfaction.

The user trustworthiness, as well as the system security, are defined by using the 'reliability' keyword here.

1. To analyze user reviews about the quality and reliability of biometric systems.

2. To assess user concerns about biometric data privacy.

3. To compare different biometric systems based on users' perspectives.

1. *Related Work:*

The traditional way of assuring safety and security password protocol systems is used. But this protocol has some drawbacks: it can be stolen, users can forget their password. As this security issue has become a talk of the topic all over the world, the UK government started using biometric traits for identification in 1960. After this several studies took place for designing biometric system and having a good recognition accuracy [8]. This technology uses the physical or behavioral traits of the user to solve the problem of authentication. Biometric system is consisting of four modules which are sensor module, feature extraction module, template database and a matching module. The process of authentication goes through in two-stage: Enrollment stage and verification stage. When a user puts his thumb on the sensor a picture of the fingerprint is taken by the sensor module. Further from this picture the system extracted some data and make it suitable to generate template data and save them in a database for the verification stage. After that, a query is made for matching the data with the template database to make sure that this user is a valid person. Imposing this for solving the security issue there arises two concerns one is biometric traits cannot be revoked and reissued when the biometric information of a person is compromised. If a person's fingerprint image is stolen it cannot be replaced in the template database as this information is unique.

Ratha [9] has detected eight points from where this biometric information can be stolen or tempered. Namely, attacks on the interface, attacks on the modules: feature extraction module and matching module, attacks on the template database and also the channels from where the biometric information is flowing. They observed, spoofing attack which is an interface-level attack occurs because of the fake biometric presentation. An experiment was taking place by attacking with the fake fingerprints. The result showing that the acceptance rate of fake fingerprint 67%. Liveness detection is a well-known countermeasure to distinguish between the fake fingerprint and the real fingerprint. Two scientists proposed to detect the perspiration phenomenon to differentiate the living fingers from the fake non – living fingers. Another researcher Coli Er Al. utilized the static feature as well as the dynamic features of a fingerprint image which to prevent the spoofing attack.

Galbally [10] proposed a method that uses fingerprint parameterization based on the quality of fingerprint images. He proposed it as a classification problem where the result will be real or fake. Kim, a researcher proposed to design an image descriptor to handle liveness detection. He used a property of image which is dispersion. The difference of dispersion in the image gradient field will be different if the fingerprint is being faked.

This accuracy of a biometric system can be measured by using three factors: False Accept Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (ERR). This accuracy depends on the image quality and the matching algorithms. There is a platform which is FVC-ongoing where the researcher can upload their matching algorithm to evaluate the FAR, FRR and ERR. At present, the best matching algorithm which name is HXKJ and ERR = 0.022% [8].

Among 4.6 billion mobile users 52.7% browse the Internet which increases cybercrimes rapidly. Bangladesh Government initiated a biometric SIM registration program in December 2015. Aim of this program has to verify the real owner of the SIM using NID and help to unearth the real criminal. S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell demonstrate about the ownership, user identity, exploitation, also security and safety concerns that challenged this program by using the method interview. Western world preserves users' privacy rights where Bangladesh is lagging behind. Their online survey concluded that 77% of participants dislike the SIM registration system. Only 15% supported and 4% ignored the survey [2].

V. Andronikou, D. S. Demetis, T. Varvarigou, I. Group, and H. Street [3] described the design complexity, security issues, personal attacks (PA), indicators and factors of biometric systems. How biometric encryption works, what concepts are identified by Electronic Privacy Information Centre (EPIC) and the panacea of those are also covered and highlighted here. The result of this study shows that more research needed to focus on technical domain and biometrics are not only the part of solution but also problem. The real-life challenges and their linkage to social, economic and political era are still untouched in this study.

Marcos [11] defined the difficulty of a biometric system with a study. To detect the vulnerability of the biometric system two situations are intensely focused. The first one is impostors try to access the system as a substitute for a real user and another one is when a person avoids his identity which is suspenseful. Sensor, Transmission Between the sensor and the Feature Extractor, Feature Extractor, Transmission of the Extracted Features, Classifier, Database, Transmission of the Database Templates to the classifier, Decision are the eight attack levels. Three main authentication methods handheld token (card, ID, passport, etc.), knowledge-based (password, PIN, etc.) and Biometrics have some advantages and drawbacks also. Biometric technologies like fingerprint, voice, iris, face reflects some vulnerabilities and there are also solutions. Data encryption and time stamp watermarking are two methods for solution. Using observation methodology, the study is conducted. Two solution techniques, encryption and watermarking are designed in the study. For watermarking, the least significant bit substitution methodology is used. Although once the data are decrypted in encryption there is no further data protection. Adobe Photoshop and Corel Draw with Digimac technology introduce information which cannot be erased without hampering the image standard & this can be fruitful for timestamp data. The final result is, these two techniques create a strong difficulty for cybercriminals to access the system for hampering the data.

By examining the existing legal and academic debates, the privacy concerns and debate of biometrics in the biometric context is a much important issue nowadays. The main motto of the study is to discuss several controversial legal issues rises from biometric context and analytical opinions conduction from the view of legal perspective on biometrics and data protection. Previous history observation methodology is used to run the study. Many countries like Norwegian, Swedish and US follow the law to protect data from a legal perspective [12]. To embrace the latest technology, government and commercial organizations play a powerful role. Many countries and entities have begun including the biometric technologies like the fingerprint reader, facial recognition and RFID chips in different sectors to resolve the unauthorized use. To minimize fraud and improve national security by using biometric technology, several legislative and regulatory initiatives have been adopted. To store information on a portable token is welcomed by a data-protection advocate but there are some security concerns still exist. By using various biometric applications many controversial legal problems arise. Biometric privacy should be protected or what extent it should be protected depends on the context in the biometric domain. On several biometric applications, major privacy concerns are attempted to explore. As a result, measuring the applicability of biometric application policies and legal laws with biometric technical elements, extension privacy on biometric context is tracked. Although the legal measures are improving with widespread implementation, they still need some clue for shaping, provided by current initiatives.

1. *Research Questions:*

The main study question is, how does the user reliability effect for adopting the biometric authentication system in Bangladesh? Also, have some sub-questions:

1. What type of biometric systems are frequently used in Bangladesh?

2. What are the security issues experienced by biometric system users?

3. What are the barriers of users to adopt a biometric system?

1. **Methodology:**

As the study focuses on user reliability and acceptance, the answer to these research questions must be solved by the user's perspective. User reliability and acceptance level can be analyzed with numeric values. So our selected data type is quantitative. To find out the final outcome some mathematical functions and data analysis tools will be used.

According to the literature section, most of the studies followed the design analysis and observation method [1] [3] [8] [11] [12]. Only S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell demonstrate the outcome using a survey [2], which is most appropriate for this reliability and acceptance study. This study will give the outcome of the user's opinion about biometric systems. Observing the systems does not give a proper result. For this study, neither the interview nor observation is appropriate.

1. *Data Collection Methods:*

The Observation method is the easiest and simplest among all the methods for data collection. Technical knowledge is not significant here. To formulate the hypothesis, observation is the foundation for collecting data. Researchers can get an accuracy of any information which cannot provide by any other data collection methods. Because in interview and questionnaire methods, researchers have to judge the study based on information provided by the participants which may not accurate sometimes. But in observation, all the information researchers can observe by checking the predefined accuracy. But sometimes researchers have some restrictions to observe the personal data. From the personal view of researchers, it can make a biased result. It also takes so much time, expenses are high and validity checking is also hard. So thinking about the drawbacks, the observation methodology is not selected for the study.

Another data collection method is an interview method. Interview, a face to face data collection approach is also suitable for the study. Despite the rising popularity of the survey method, an interview also maintains the popularity because a face to face data collection decreases the false statement from the participants like gender, age, etc. Accurate screening is a good factor here. Non -verbal questions can be captured here because body language is also seen by the researchers. Participant’s focus, emotions, behaviors can be captured by this method. No disturbance cannot occur during the interview but in survey or observation methods texting messages, mail checking, web surfing, video streaming, etc. obstacles maybe rise. But the cost is also high because it needs technical devices to collect data like a recorder, video camera, etc. sometimes it is difficult to manage participants for interviews. Taking Permission for the record the speech may be troublesome for researchers. Collecting a large amount of information may be difficult. Much time needed for taking interviews as time, date, place fixing kills a huge amount of time. For time shortage the interview method is avoided for the study. As the study is for general users, so the method is not appropriate for the data collection.

For this quantitative study, questionnaires are more applicable rather than an interview, observation, discussion or other methods. It collects public opinion and gives a suitable result that can help to visualize any problem easily. It is cost-effective and time-consuming. The user's aptitude, consciousness, and opinion is the main agenda here. If this study conduct with security issues and the data alignment work, then company opinion i.e. Grameenphone customer service, NID issue office, has to be considered. But this study works with the reliability of users and how they feel about adopting a biometric system as security is the concern here. Although less data accuracy, missing data, meaningless response etc. are some drawbacks, it’s an acceptable method for the study. Many researchers, previously collect the data using other methods but the questionnaire method is suitable and best for the study.

We will use ‘Internet Survey’ for this study. It deals with public opinion and gives a suitable result that can help to visualize any problem easily. The online survey is comparatively time savior, free of cost and helps to gather a huge amount of targeted data.

1. *Participants/Sampling:*

The study focus on users of biometric systems. So the participates of our survey will be general people with random ages and gender who uses the biometric system for identity verification.

1. *Research Ethics:*

As we collect users’ personal opinions about a security system, so we must ensure data privacy. All the personal information will be secured and will never be exposed. It will take 15 to 20 min to complete our survey.

1. *Data Collection strategy:*

The strategy of collecting data by using questionnaires to get measurable data that can be aligned. The question will be made out of the aim such that the aim of the research will fulfill. This method is an effective research method because the whole process will be done using the internet. As the whole process becomes autonomous, it eliminates the human error factor [13].

In this strategy, we are choosing the random selection of data collection among the citizen of our country. The data collection method for random selection for citizens would have been selected within the age of 18-50 years and then the questionnaires will be distributed among 200-300 citizens [13]. It is obvious that if more citizen does the questionnaires better result will come out and we will be able to give a good outcome of our research study. The best solution will be if we can provide questionnaires to all the citizen and that will be the representation of a country situation regarding our research problem. But this cannot be done because of the short time period of the task. The questionnaires will have a little problem to determine our research aim and objective. The human factor which refers to if all the chosen citizen does not understand the questions or they do not answer at all.

This data collection method will not be sent to the citizen which are below 18 years old or 50 years old. Because the person who is not among 18 – 50 years old tends to be children or elder person. Their opinion about our research study is not countable because they cannot understand the problem of our research study. The reason why we are choosing 18 – 50 years old people is they are more familiar with the technology of modern times. We will make sure that the information of the participant will remain anonymous. This data will not be saved after this study is done. We will provide enough information about the research aims and objectives and the research problem to our participants [13].

1. **References:**

[1] R. E. O. Paderes, “A Comparative Review of Biometric Security Systems,” *Proc. - 8th Int. Conf. Bio-Science Bio-Technology, BSBT 2015*, pp. 8–11, 2016.

[2] S. I. Ahmed, M. R. Hoque, S. Guha, M. R. Rifat, and N. Dell, “Privacy, security, and surveillance in the global south: A study of biometric mobile SIM registration in Bangladesh,” *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 2017-May, pp. 906–918, 2017.

[3] V. Andronikou, D. S. Demetis, T. Varvarigou, I. Group, and H. Street, “Biometric Implementations and the Implications for Security and Privacy,” *1st in-house FIDIS J. Issue*, no. 1, pp. 1–20, 2007.

[4] “Standard Chartered Bank - Touch Registration and Login.” [Online]. Available: https://www.online-banking.standardchartered.com/login/IBank?ser=100&act=TouchIdRegistration.jsp&cntry=BD. [Accessed: 24-Sep-2019].

[5] “Bangladesh Introduces ‘Smart’ National Identity Cards - Global Voices Advox.” [Online]. Available: https://advox.globalvoices.org/2016/10/07/bangladesh-introduces-smart-national-identity-cards/. [Accessed: 24-Sep-2019].

[6] “Joy launches NID verification gateway server | Dhaka Tribune.” [Online]. Available: https://www.dhakatribune.com/bangladesh/government-affairs/2019/07/17/joy-to-launch-nid-verification-gateway. [Accessed: 24-Sep-2019].

[7] “Global Biometric System Market Research Report- Forecast 2023 | MRFR.” [Online]. Available: https://www.marketresearchfuture.com/reports/biometric-system-market-3754. [Accessed: 24-Sep-2019].

[8] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and accuracy of fingerprint-based biometrics: A review,” *Symmetry (Basel).*, vol. 11, no. 2, 2019.

[9] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[10] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, “A high performance fingerprint liveness detection method based on quality related features,” *Futur. Gener. Comput. Syst.*, vol. 28, no. 1, pp. 311–321, Jan. 2012.

[11] M. Faúndez-Zanuy, “On the vulnerability of biometric security systems,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 19, no. 6, pp. 3–8, 2004.

[12] Y. Liu, “Identifying legal concerns in the biometric context,” *J. Int. Commer. Law Technol.*, vol. 3, no. 1, pp. 45–54, 2008.

[13] Martyn Denscombe, “The Good Research Guide for small-scale social research projects,” *Open Univ. Press. McGraw-Hill Educ.*, vol. Fourth Edi, pp. 7–200, 2012.

# **Informed Consent Form**

We are conducting a research study titled “User Reliability and Acceptance of Biometric Systems in Bangladesh”. This study is supervised by our Faculty Advisor “Rashedul Amin Tuhin” Senior Lecturer, Department of Computer Science & Engineering, East West University.

Researchers:

Shaykh Siddique ([shaykhsiddiqee@gmail.com](mailto:(shaykhsiddiqee@gmail.com)))

Mushfiqul Alam ([alammushfiqul366@gmail.com](mailto:alammushfiqul366@gmail.com))

Monica Yasmin Momo ([y.monicamym@gmail.com](mailto:y.monicamym@gmail.com))

Tasnova Bintee Taher ([tasnovafabi@gmail.com](mailto:tasnovafabi@gmail.com))

We are asking for your voluntary participation in our research study for exploring how user reliability is effecting the acceptance of biometric authentication systems. Please read the following information about the project. If you would like to participate, please sign in the appropriate space below. If you have any further questions about this study, feel free to contact the researcher.

# **Information about the research**

The purpose of this research study is to evaluate which biometric system is more efficient and acceptable to the user in the context of user reliability and satisfactoriness of the biometric system. The analysis will be based on the description of the citizen of Bangladesh about how many problems they face when they are using a biometric authentication system. By a questionnaire, we will try to determine the efficiency and acceptance of a biometric system.

# **Participating in the study**

|  |  |
| --- | --- |
| If you participate, you will be asked to: | Provide answers to a questionnaire regarding your experience using a biometric authentication system. |
| The time required for participation: | Approximately 15 – 20 minutes. |
| Potential Risks of this study: | There is no anticipated discomfort for those contributing to this study, so the risk to participants is minimal. |
| Benefits: | You will be personally benefitted from taking part in this study because we are going to determine which biometric system is efficient and easy to use for you. However, you may receive a copy of the final report upon request. |
| How confidentially will be maintained: | Your given information will be kept confidential and will not be released without your consent except as required by law. Your signed consent form will be stored separately from the data. |

# **Voluntary Participation:**

Participation in this study is completely voluntary. If you decide not to participate there will be no negative effect. Please be aware that if you decided to participate, you may stop participating at any time and may decide not to answer any specific question.

By signing this form, I am attesting that I have read and understood the information above and I freely give me consent to participate.

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Name of Participant | Date and Signature |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Name of Researcher | Date and Signature |

# **Data Collection Protocol**

Questionnaire

1. How frequently you use the biometric authentication system? (O1)

Here, 1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always

Question 2, 3, and 4 from the following scenario:

Mobile phones and other devices have features of biometric authentication to improve identification security. “Fingerprint”, “face scan” are very popular in this case. Also, the National Identification Services, Mobile Phone Companies, Online Banks have biometric data storage.

1. Do you think it is possible to steal your biometric data from these kinds of services? (O2)

Strongly Disagree/ Disagree/ Neutral/ Agree/ Strongly Agree.

1. Do you think you have enough privilege to update/ change/ remove/modify your personal data from phones or personal gadgets? (O1)

Strongly Disagree/ Disagree/ Neutral/ Agree/ Strongly Agree.

1. To update/ change/ remove/modify your personal data from NID databases, Mobile phone Company data storage, do you have enough privilege? (O1)

Strongly Disagree/ Disagree/ Neutral/ Agree/ Strongly Agree.

1. The biometric system works on body measurement. If anything goes wrong with your skin, voice or physical any injury biometric system cannot verify you. In that case rate the system reliability(O3)-

Physical

Face scan – Low/ Medium/High

Fingerprint scan - Low/ Medium/High

Hand palm scan - Low/ Medium/High

Iris scan - Low/ Medium/High

DNA test - Low/ Medium/High

Behavioral

Typing keystroke - Low/ Medium/High

Signature validation - Low/ Medium/High

Voice detection - Low/ Medium/High

1. If any reason, you are failed to access the biometric security system what kind of secondary mechanism (recovery option) you prefer to use? (O2)

Multi-Biometric Authentication

Password/Pin

Recovery Email/Massage

Other add here

1. In Sic-fiction movies, we see the thief took the victim’s fingerprints or make the victim unconscious and collect biometric information. Do you think it’s possible in real life? (O2)

Never/Rarely/Sometimes/Often/Always

1. On the basis of your use, which biometric authentication technique would you prefer most? (O3)

Physical

Face scan – Low/ Medium/High

Fingerprint scan - Low/ Medium/High

Hand palm scan - Low/ Medium/High

Iris scan - Low/ Medium/High

DNA test - Low/ Medium/High

Behavioral

Typing keystroke - Low/ Medium/High

Signature validation - Low/ Medium/High

Voice detection - Low/ Medium/High

1. On basic of your security which biometric authentication technique would you prefer most? (O3)

Physical

Face scan – Low/ Medium/High

Fingerprint scan - Low/ Medium/High

Hand palm scan - Low/ Medium/High

Iris scan - Low/ Medium/High

DNA test - Low/ Medium/High

Behavioral

Typing keystroke - Low/ Medium/High

Signature validation - Low/ Medium/High

Voice detection - Low/ Medium/High

1. What are the most common issues you faced? (O1)

Hardware Failure - Never/Rarely/Sometimes/Often/Always

Vulnerable Software - Never/Rarely/Sometimes/Often/Always

Vulnerable Data Storage - Never/Rarely/Sometimes/Often/Always

Authorization Failure for real person - Never/Rarely/Sometimes/Often/Always

1. If you face other problems but not mentioned here, then what is that and how frequent? (O1)

Write your answer here.

1. Do you think, your biometric information can be leaked/taken without permission for software weakness? (O1)

Strongly Disagree/ Disagree/ Neutral/ Agree/ Strongly Agree.

1. What do you think, will be the main fact to buy a new biometric security system? (O3)

User-friendly - Never/Rarely/Sometimes/Often/Always

Strong Security - Never/Rarely/Sometimes/Often/Always

Price - Never/Rarely/Sometimes/Often/Always

Depends on the environment of use - Never/Rarely/Sometimes/Often/Always

1. Do you ever use any third-party applications that need/store biometric information? (O2)

Never/Rarely/Sometimes/Often/Always

1. Do you think all kinds of biometric systems have well-defined Terms and Conditions? (O2)

Strongly Disagree/ Disagree/ Neutral/ Agree/ Strongly Agree.

1. Do you read all Terms and Conditions before using a biometric system? (O2)

Never/Rarely/Sometimes/Often/Always

1. Do you think instead of using a password/pin based security system, the biometric system can give more security to users? (O1)

Strongly Disagree/ Disagree/ Neutral/ Agree/ Strongly Agree.